CLAIMS

What is claimed is:

1. In a network comprising a first electronic device and a second electronic device, a method for authenticating access to a controlled network, said method comprising:

a) authenticating said second electronic device to said first electronic device, said first electronic device communicatively coupled to said second electronic device;

b) authenticating said first electronic device to said second electronic device;

c) determining a key at said first electronic device and at said second electronic device; and

d) authenticating a user to a central authentication server.

2. The method of Claim 1 wherein said first electronic device is a client device and said second electronic device is a network device.

3. The method of Claim 2 wherein said step a) comprises:

receiving a first message from said client device at said network device, said first message comprising a device identifier and a first random number;

receiving a second message from said network device at said client device, said second message comprising a second random number and a first digest, said first digest comprising a one-way hash function operating on said first random number, said device identifier, and a first secret shared between said network device and said client device;

determining a second digest at said client device, said second digest comprising a one-way hash function operating on said first random number, said device identifier, and said first secret;

comparing said first digest to said second digest at said client device; and

provided said first digest matches said second digest, authenticating said network device to said client device.

4. The method of Claim 2 wherein said step b) comprises:

receiving a third message from said client device at said network device, said third message comprising a third digest, said third digest comprising a one-way hash function operating on said second random number, said device identifier, and said first secret;

determining a fourth digest at said network device, said fourth digest comprising said second random number, said device identifier, and said first secret;

comparing said third digest to said fourth digest at said client device; and

provided said third digest matches said fourth digest, authenticating said client device to said network device.

5. The method as recited in Claim 2 wherein step c) comprises:

determining a fifth digest at said network device, said fifth digest comprising said device identifier received from said client device, said first secret, said first random number, and said second random number, said fifth digest from which said network device selects bits and determines said key; and

calculating a sixth digest at said client device, said sixth digest comprising said device identifier, said first secret, said first random number and said second random number, said sixth digest from which said client device selects bits and determines said key.

6. The method as recited in Claim 2 wherein said step d) comprises:

transmitting a request for a user_name and a user_credentials to said client device.

sending said user_name and said user_credentials to said network device from said client device;

forwarding said user_name and said user_credentials to said central authentication server from said network device; and

employing said user_name and said user_credentials for authenticating said user at said central authentication server.

7. The method as recited in Claim 6 further comprising:

provided said user is authenticated at said central authentication server:

sending a success message to said network device at said central authentication server;

forwarding said success message to said client device at said network device;

allowing said client device to access said controlled network at said network device; and

provided said user is not authenticated at said central authentication server:

sending a failure message to said network device at said central authentication server;

forwarding said failure message to said client device at said network device;

disallowing said client device access to said controlled network at said network device.

8. The method as recited in Claim 1 wherein said first electronic device is a client device and said second electronic device is a central authentication server.

9. The method of Claim 8 wherein a network device is employed for providing an interface between said client device and said central authentication server.

10. The method of Claim 9 wherein step a) comprises:

receiving a first standard message from said client device at said network device;

forwarding said first standard message to said central authentication server at said network device; and

receiving said first standard message from said network device at said central authentication server whereby said client device is identified to said central authentication server.

11. The method as recited in Claim 10 further comprising:

sending a second standard message to said network device from said central authentication server; and

forwarding said second standard message to said client device from said network device, whereby said central authentication server is authenticated to said client device.

12. The method as recited in Claim 10 wherein said step c) comprises:

sending a third standard message to said network device from said client device; and

forwarding said third standard message to said central authentication server from said network device, whereby said client device is authenticated to said central authentication server.

13. The method as recited in Claim 10 wherein said first standard message comprises a standard EAP-TLS protocol message.

14. The method as recited in Claim 11 wherein said second standard message comprises a key exchange from said central authentication server to said client device.

15. The method as recited in Claim 11 wherein said second standard message comprises a standard EAP-TLS protocol message.

16. The method as recited in Claim 12 wherein said third standard message comprises a key exchange from said client device to said central authentication server.

17. The method as recited in Claim 12 wherein said third standard message comprises a standard EAP-TLS protocol message.

18. The method as recited in Claim 1 wherein said first electronic device and said second electronic device are communicatively coupled by a wireless connection.

19. The method as recited in Claim 1 wherein said first electronic device and said second electronic device are communicatively coupled by a wired connection.

20. The method as recited in Claim 2 wherein said network device is a wireless network access point.

21. A computer system network comprising:

a central authentication server for authenticating a user to send or receive information over a computer system network;

a first electronic device coupled to said network device; and

a second electronic device coupled to said central authentication server;

said central authentication server, said first electronic device and said second electronic device operating in conjunction to perform a method of authenticating access to a controlled network, said method comprising:

a) authenticating said second electronic device to said first electronic device, said first electronic device communicatively coupled to said second electronic device;

b) authenticating said first electronic device to said second electronic device;

c) determining a key at said first electronic device and at said second electronic device; and

d) authenticating a user to a central authentication server.

22. The method of Claim 21 wherein said first electronic device is a client device and said second electronic device is a network device.

23. The method of Claim 22 wherein said step a) comprises:

receiving a first message from said client device at said network device, said first message comprising a device identifier and a first random number;

receiving a second message from said network device at said client device, said second message comprising a second random number and a first digest, said first digest comprising a one-way hash function operating on said first random number, said device identifier, and a first secret shared between said network device and said client device;

determining a second digest at said client device, said second digest comprising a one-way hash function operating on said first random number, said device identifier, and said first secret;

comparing said first digest to said second digest at said client device; and

provided said first digest matches said second digest, authenticating said network device to said client device.

24. The method of Claim 22 wherein said step b) comprises:

receiving a third message from said client device at said network device, said third message comprising a third digest, said third digest comprising a one-way hash function operating on said second random number, said device identifier, and said first secret;

determining a fourth digest at said network device, said fourth digest comprising said second random number, said device identifier, and said first secret;

comparing said third digest to said fourth digest at said client device; and

provided said third digest matches said fourth digest, authenticating said client device to said network device.

25. The method as recited in Claim 22 wherein step c) comprises:

determining a fifth digest at said network device, said fifth digest comprising said device identifier received from said client device, said first secret, said first random number, and said second random number, said fifth digest from which said network device selects bits and determines said key; and

calculating a sixth digest at said client device, said sixth digest comprising said device identifier, said first secret, said first random number and said second random number, said sixth digest from which said client device selects bits and determines said key.

26. The method as recited in Claim 22 wherein said step d) comprises:

transmitting a request for a user_name and a user_credentials to said client device.

sending said user_name and said user_credentials to said network device from said client device;

forwarding said user_name and said user_credentials to said central authentication server from said network device; and

employing said user_name and said user_credentials for authenticating said user at said central authentication server.

27. The method as recited in Claim 26 further comprising:

provided said user is authenticated at said central authentication server:

sending a success message to said network device at said central authentication server;

forwarding said success message to said client device at said network device;

allowing said client device to access said controlled network at said network device; and

provided said user is not authenticated at said central authentication server:

sending a failure message to said network device at said central authentication server;

forwarding said failure message to said client device at said network device;

disallowing said client device access to said controlled network at said network device.

28. The method as recited in Claim 21 wherein said first electronic device is a client device and said second electronic device is a central authentication server.

29. The method of Claim 28 wherein a network device is employed for providing an interface between said client device and said central authentication server.

30. The method of Claim 29 wherein step a) comprises:

receiving a first standard message from said client device at said network device;

forwarding said first standard message to said central authentication server at said network device; and

receiving said first standard message from said network device at said central authentication server whereby said client device is identified to said central authentication server.

31. The method as recited in Claim 30 further comprising:

sending a second standard message to said network device from said central authentication server; and

forwarding said second standard message to said client device from said network device, whereby said central authentication server is authenticated to said client device.

32. The method as recited in Claim 30 wherein said step c) comprises:

sending a third standard message to said network device from said client device; and

forwarding said third standard message to said central authentication server from said network device, whereby said client device is authenticated to said central authentication server.

33. The method as recited in Claim 30 wherein said first standard message comprises a standard EAP-TLS protocol message.

34. The method as recited in Claim 31 wherein said second standard message comprises a key exchange from said central authentication server to said client device.

35. The method as recited in Claim 31 wherein said second standard message comprises a standard EAP-TLS protocol message.

36. The method as recited in Claim 32 wherein said third standard message comprises a key exchange from said client device to said central authentication server.

37. The method as recited in Claim 32 wherein said third standard message comprises a standard EAP-TLS protocol message.

38. The method as recited in Claim 21 wherein said first electronic device and said second electronic device are communicatively coupled by a wireless connection.

39. The method as recited in Claim 21 wherein said first electronic device and said second electronic device are communicatively coupled by a wired connection.

40. The method as recited in Claim 22 wherein said network device is a wireless network access point.

41. In a computer-usable medium having computer-readable program code embodied therein, a computer-implemented method for authenticating a first electronic device and a second electronic device, said method comprising:

a) authenticating said second electronic device to said first electronic device, said first electronic device communicatively coupled to said second electronic device;

b) authenticating said first electronic device to said second electronic device;

c) Determining a key at said first electronic device and at said second electronic device; and

d) authenticating a user to a central authentication server.

42. The computer implemented method of Claim 41 wherein said first electronic device is a client device and said second electronic device is a network device.

43. The computer implemented method of Claim 42 wherein said step a) comprises:

receiving a first message from said client device at said network device, said first message comprising a device identifier and a first random number;

receiving a second message from said network device at said client device, said second message comprising a second random number and a first digest, said first digest comprising a one-way hash function operating on said first random number, said device identifier, and a first secret shared between said network device and said client device;

determining a second digest at said client device, said second digest comprising a one-way hash function operating on said first random number, said device identifier, and said first secret;

comparing said first digest to said second digest at said client device; and

provided said first digest matches said second digest, authenticating said network device to said client device.

44. The computer implemented method of Claim 42 wherein said step b) comprises:

receiving a third message from said client device at said network device, said third message comprising a third digest, said third digest comprising a one-way hash function operating on said second random number, said device identifier, and said first secret;

determining a fourth digest at said network device, said fourth digest comprising said second random number, said device identifier, and said first secret;

comparing said third digest to said fourth digest at said client device; and

provided said third digest matches said fourth digest, authenticating said client device to said network device.

45. The computer implemented method as recited in Claim 42 wherein step c) comprises:

determining a fifth digest at said network device, said fifth digest comprising said device identifier received from said client device, said first secret, said first random number, and said second random number, said fifth digest from which said network device selects bits and determines said key; and

calculating a sixth digest at said client device, said sixth digest comprising said device identifier, said first secret, said first random number and

said second random number, said sixth digest from which said client device selects bits and determines said key.

46. The computer implemented method as recited in Claim 42 wherein said step d) comprises:

transmitting a request for a user_name and a user_credentials to said client device.

sending said user_name and said user_credentials to said network device from said client device;

forwarding said user_name and said user_credentials to said central authentication server from said network device; and

employing said user_name and said user_credentials for authenticating said user at said central authentication server.

47. The computer implemented method as recited in Claim 46 further comprising:

provided said user is authenticated at said central authentication server:

sending a success message to said network device at said central authentication server;

forwarding said success message to said client device at said network device;

allowing said client device to access said controlled network at said network device; and

provided said user is not authenticated at said central authentication server:

sending a failure message to said network device at said central authentication server;

forwarding said failure message to said client device at said network device;

disallowing said client device access to said controlled network at said network device.

48. The computer implemented method as recited in Claim 41 wherein said first electronic device is a client device and said second electronic device is a central authentication server.

49. The computer implemented method of Claim 48 wherein a network device is employed for providing an interface between said client device and said central authentication server.

50. The computer implemented method of Claim 49 wherein step a) comprises:

receiving a first standard message from said client device at said network device;

forwarding said first standard message to said central authentication server at said network device; and

receiving said first standard message from said network device at said central authentication server whereby said client device is identified to said central authentication server.

51. The computer implemented method as recited in Claim 50 further comprising:

sending a second standard message to said network device from said central authentication server; and

forwarding said second standard message to said client device from said network device, whereby said central authentication server is authenticated to said client device.

52. The computer implemented method as recited in Claim 50 wherein said step c) comprises:

sending a third standard message to said network device from said client device; and

forwarding said third standard message to said central authentication server from said network device, whereby said client device is authenticated to said central authentication server.

53. The computer implemented method as recited in Claim 50 wherein said first standard message comprises a standard EAP-TLS protocol message.

54. The computer implemented method as recited in Claim 51 wherein said second standard message comprises a key exchange from said central authentication server to said client device.

55. The computer implemented method as recited in Claim 51 wherein said second standard message comprises a standard EAP-TLS protocol message.

56. The computer implemented method as recited in Claim 52 wherein said third standard message comprises a key exchange from said client device to said central authentication server.

57. The computer implemented method as recited in Claim 52 wherein said third standard message comprises a standard EAP-TLS protocol message.

58. The computer implemented method as recited in Claim 41 wherein said first electronic device and said second electronic device are communicatively coupled by a wireless connection.

59. The computer implemented method as recited in Claim 41 wherein said first electronic device and said second electronic device are communicatively coupled by a wired connection.

60. The computer implemented method as recited in Claim 42 wherein said network device is a wireless network access point.